PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-176637
(43)Date of publication of application : 21.06.2002

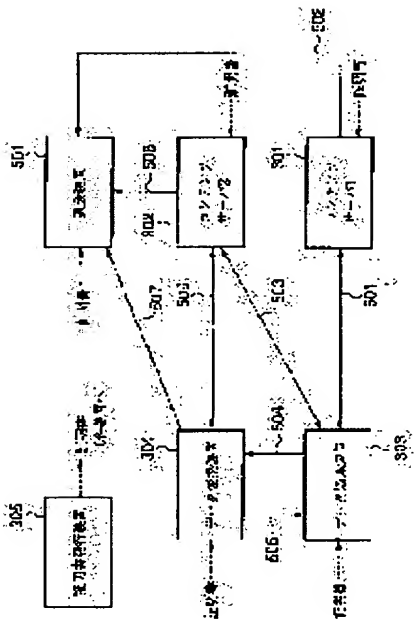
(51)Int.Cl. H04N 7/173
G06F 15/00
G06F 17/30
G06F 17/60

(21)Application number : 2000-370345
(22)Date of filing : 05.12.2000

(71)Applicant : CANON INC
(72)Inventor : WAKAO SATOSHI

(54) DATA DISTRIBUTION METHOD AND ITS SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data distribution method and a data distribution system that can automatically impose charging on a user accompanying acquisition and conversion of contents data by the user, in addition to the authentication of the user.
SOLUTION: The data distribution system is configured, with at least a user terminal 303 and contents servers 301, 302 being interconnected via a network and the contents servers distributes contents data to the user terminal upon the request of the user terminal 303. The data distribution server is provided with a certificate issue device 305, that is connected to the user terminal and the contents servers via the network and issues digital identification information to the user terminal and the contents servers, with a data converter 304 that converts the content data into data, in a form that can be processed by the user terminal, and a charging device 501 that conducts charging corresponding to the distribution of the contents data and the conversion of the contents data upon the request from the contents servers and the data converter. The user terminal 303, the data converter 304 and the charging device 501 carry out transmission reception, only when mutual authentication on the basis of the digital identification information from the certificate issue device 305 is successful.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－176637
（P2002－176637A）
(43)公開日　平成14年６月21日(2002.6.21)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｈ０４Ｎ	7/173	６４０	Ｈ０４Ｎ　7/173	６４０Ａ	５Ｂ０７５
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｚ	５Ｂ０８５
	17/30	１１０	17/30	１１０Ｆ	５Ｃ０６４
		２４０		２４０Ｃ	
	17/60	ＺＥＣ	17/60	ＺＥＣ	

審査請求　未請求　請求項の数17　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願2000－370345(P2000－370345)

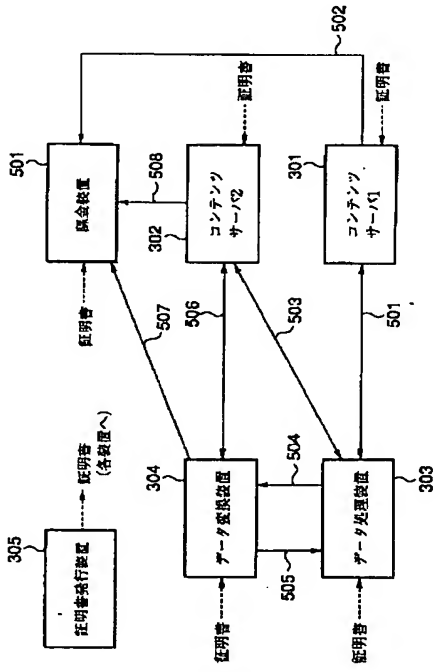
(22)出願日　平成12年12月５日(2000.12.5)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　若尾　聡
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100076428
弁理士　大塚　康徳　（外２名）

Ｆターム(参考)　5B075 PQ02 PQ04 PQ05
5B085 AC04 AE23 BG07
5C064 BA01 BA07 BB01 BB07 BC01
BC07 BC16 BC18 BC20 BC23
BD02 BD08

(54)【発明の名称】　データ配信方法及びそのシステム

(57)【要約】
【課題】　ユーザの認証に加えて、そのユーザによるコンテンツデータの取得及びデータ変換に伴う課金を自動的に行う。
【解決手段】　少なくともユーザ端末３０３とコンテンツサーバ３０１，３０２とがネットワークを介して接続され、ユーザ端末３０３からの要求によりコンテンツサーバからユーザ端末にコンテンツデータを配信するデータ配信システムであって、ネットワーク介して接続され、ユーザ端末及びコンテンツサーバに対してディジタル識別情報を発行する証明書発行装置３０５と、ユーザ端末３０３からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置３０４と、コンテンツサーバ及びデータ変換装置からの要求に応じて、コンテンツデータの配信及びコンテンツデータの変換に対応する課金を行う課金装置５０１とを有し、ユーザ端末３０３、データ変換装置３０４及び課金装置５０１は、認証装置３０５からのディジタル識別情報に基づく相互認証に成功した場合にのみ送受信する。



1

【特許請求の範囲】

【請求項１】　少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムであって、

前記ネットワーク介して接続され、前記ユーザ端末及びコンテンツサーバに対してディジタル識別情報を発行する認証装置と、

前記ユーザ端末からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置と、

前記コンテンツサーバ及び前記データ変換装置からの要求に応じて、前記コンテンツデータの配信及び前記コンテンツデータの変換に対応する課金を行う課金装置とを有し、

前記ユーザ端末、前記データ変換装置及び前記課金装置は、前記認証装置からの前記ディジタル識別情報に基づく相互認証に成功した場合に送受信することを特徴とするデータ配信システム。

【請求項２】　前記ユーザ端末は、前記コンテンツサーバに要求した前記コンテンツデータが当該ユーザ端末で処理不可能な場合、前記データ変換装置に対して当該コンテンツデータを、当該ユーザ端末が処理可能な形式のデータに変換するように要求することを特徴とする請求項１に記載のデータ配信システム。

【請求項３】　前記課金装置は、

課金を行うため必要となるデータを前記コンテンツサーバ及び前記データ変換装置から受信する受信手段と、

前記受信手段により受信された前記データに基づいて課金データを生成する課金データ生成手段と、

前記課金データを登録する課金データベースと、を有することを特徴とする請求項１又は２に記載のデータ配信システム。

【請求項４】　前記認証装置は更に、

前記ユーザ端末、前記コンテンツサーバ及び前記データ変換装置からのディジタル識別データ発行要求を受信する受信手段と、

前記受信手段により受信された発行要求を送信した前記ユーザ端末、前記コンテンツサーバ又は前記データ変換装置に対してディジタル識別データを発行するかどうかを判断する判断手段と、

前記判断手段により発行すると判断された前記ユーザ端末、前記コンテンツサーバ又は前記データ変換装置に対する前記ディジタル識別データを発行する発行手段と、

前記ディジタル識別データを登録する登録手段と、

前記発行手段により発行されたディジタル識別データを当該前記ユーザ端末、前記コンテンツサーバ又は前記データ変換装置に送信する手段と、を有することを特徴とする請求項１に記載のデータ配信システム。

2

【請求項５】　前記コンテンツデータは、ＭＰＥＧデータであることを特徴とする請求項１乃至４のいずれか１項に記載のデータ配信システム。

【請求項６】　前記認証装置は、更に、

前記登録手段に登録された前記ディジタル識別データを無効化する指示を受信すると、前記登録手段に登録された、対応するディジタル識別データを削除することを特徴とする請求項４に記載のデータ配信システム。

【請求項７】　少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムにおけるデータ配信方法であって、

前記ネットワーク介して接続され、前記ユーザ端末及びコンテンツサーバに対してディジタル識別情報を発行する工程と、

前記ユーザ端末からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置によりデータを変換する工程と、

前記コンテンツサーバ及び前記データ変換装置からの要求に応じて、前記コンテンツデータの配信及び前記コンテンツデータの変換に対応する課金を課金装置により行わせる課金工程とを有し、

前記ユーザ端末、前記データ変換装置及び前記課金装置は、前記ディジタル識別情報に基づく認証に成功した場合に送受信することを特徴とするデータ配信方法。

【請求項８】　前記ユーザ端末は、前記コンテンツサーバに要求した前記コンテンツデータが当該ユーザ端末で処理不可能な場合、前記データ変換装置に対して当該コンテンツデータを、当該ユーザ端末が処理可能な形式のデータに変換するように要求することを特徴とする請求項７に記載のデータ配信方法。

【請求項９】　前記課金工程で、

課金を行うため必要となるデータを前記コンテンツサーバ及び前記データ変換装置から受信する受信工程と、

前記受信工程で受信された前記データに基づいて課金データを生成する課金データ生成工程と、を有することを特徴とする請求項７又は８に記載のデータ配信方法。

【請求項１０】　前記ディジタル識別情報は、

前記ユーザ端末、前記コンテンツサーバ及び前記データ変換装置からのディジタル識別データ発行要求に基づいて発行されることを特徴とする請求項７に記載のデータ配信方法。

【請求項１１】　前記コンテンツデータは、ＭＰＥＧデータであることを特徴とする請求項７乃至１０のいずれか１項に記載のデータ配信方法。

【請求項１２】　前記ディジタル識別データを無効化する指示を受信すると対応するディジタル識別データを削除する工程を更に有することを特徴とする請求項７に記載のデータ配信方法。

【請求項１３】　少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムにおけるデータ配信方法であって、
前記ユーザ端末及びコンテンツサーバからの要求に応じて、各対応するディジタル識別情報を発行する工程と、
前記ユーザ端末から前記コンテンツサーバに対してコンテンツデータを要求する工程と、
前記要求に応じて前記コンテンツサーバから、要求したユーザ端末に前記コンテンツデータを送信する送信工程と、
前記コンテンツデータが前記ユーザ端末が処理可能な形式のデータでない場合に、当該ユーザ端末が処理可能なデータ形式のデータに変換するデータ変換工程と、
前記コンテンツデータの配信及び前記コンテンツデータのデータ変換に対応する課金を行う課金工程とを有し、
前記送信工程、前記データ変換工程及び前記課金工程は、前記ディジタル識別情報に基づく認証に成功した場合に実施されることを特徴とするデータ配信方法。
【請求項１４】　前記課金工程では、
課金を行うため必要となるデータを前記コンテンツサーバ及び前記データ変換工程から取得する取得工程と、
前記取得工程で取得された前記データに基づいて課金データを生成する課金データ生成工程と、
前記課金データを課金データベースに登録する工程と、
を有することを特徴とする請求項１３に記載のデータ配信方法。
【請求項１５】　前記ネットワークに接続された各端末、サーバ及び装置に対応する前記ディジタル識別データは、それぞれ対応する各端末、サーバ及び装置からの発行要求に基づいて発行されることを特徴とする請求項１３に記載のデータ配信方法。
【請求項１６】　前記コンテンツデータは、ＭＰＥＧデータであることを特徴とする請求項１３乃至１５のいずれか１項に記載のデータ配信方法。
【請求項１７】　各端末、サーバ及び装置に対応する前記ディジタル識別データを無効化する工程を更に有することを特徴とする請求項１３に記載のデータ配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークを介して接続されたユーザ端末からのコンテンツデータの要求に基づいて、コンテンツデータを各ユーザ端末に配信するデータ配信方法及びそのシステムに関するものである。
【０００２】
【従来の技術】近年、動画像や音声などのデータを符号化し、それぞれの符号化データをオブジェクトとして扱い、これら所謂マルチメディアデータを組み合わせて単

一のビットストリームとして伝送する手法として、ＩＳＯにてＭＰＥＧ－４(Moving Picture Experts Group pahse4)が標準化されつつある。このＭＰＥＧ－４により符号化されたコードを受信して復号する受信側（再生側）では、例えば、音声と動画シーンとを関連付けて再生する。このようなＭＰＥＧ－４コードを処理するシステムにおいては、データがオブジェクトとして扱われるという特性のために、受信したビットストリームを、オブジェクト毎に１つ１つバラバラにして容易に再編成できる。上述したようなＭＰＥＧ－４のデータストリームでは、これまでの一般的なマルチメディアストリームとは異なり、いくつもの動画シーンや動画オブジェクトを、単一のストリーム上でそれぞれ独立して送受信することができる。また音声についても同様に、いくつものオブジェクトを単一のストリーム上で独立して送受信する機能を有する。
【０００３】これらのオブジェクトを合成して、あるシーンを合成するための情報としてＶＲＭＬ(Virtual Reality Modeling Language)を修正したシーン記述情報（ＢＩＦＳ：Binary Format For Scenes）が存在する。このＢＩＦＳは、シーン記述情報が２値で記述されているもので、このＢＩＦＳに従って各シーンが合成される。このような、シーンの合成に必要な個々のオブジェクトは夫々、個別に最適な符号化が行われて送信されることになるので、復号側でも個別に復号され、ＢＩＦＳの記述に従い、個々のデータの持つ時間軸を再生装置内部の時間軸に同期させてシーンを合成、出力することになる。
【０００４】又、供給されるオブジェクトを復号装置が、そのオブジェクトを復号して再生される音声や映像を視聴する権利を有しているか否かが、伝送されるＩＰＭＰ(Intellectual Property Management and Protection)情報に基づいて判断される。
【０００５】
【発明が解決しようとする課題】このように、一般の著作権管理システムでは、ＩＰＭＰデータを用いることにより、コンテンツの不正な使用を防止することを可能にしている。しかし、コンテンツ使用に対する正当な対価を著作権者に支払う仕組みではない。この支払い（課金管理）を実現させるためには、誰がいつどんなコンテンツをどれだけ入手したかを把握するとともに、本当にその本人が入手を行ったのかを確認する（ユーザ認証）必要がある。
【０００６】コンテンツの著作権者としては、上記のような不正防止及び課金管理等を含むシステムがあれば安心してコンテンツを提供することができるが、このようなシステムが無い場合には、コンテンツを提供することを躊躇することになる。即ち、ユーザ認証や課金システムを実現することは、ネットワークを使用したコンテンツ配信サービスのビジネスを立ち上げるため必要なもの

である。しかしながら上記のデータ変換システム及びＩＰＭＰシステムと連携したユーザ認証、課金システムは考えられていなかった。

【０００７】本発明は上記従来例に鑑みてなされたもので、ユーザの認証に加えて、そのユーザによるコンテンツデータの取得及びデータ変換に伴う課金を自動的に行うことができるデータ配信方法及びシステムを提供することを目的とする。

【０００８】又本発明の目的は、視聴を許可されたユーザだけがそのコンテンツデータを使用でき、かつ自動的に、そのユーザによるコンテンツデータの使用料を課金できるデータ配信方法及びシステムを提供することにある。

【０００９】

【課題を解決するための手段】上記目的を達成するために本発明のデータ配信システムは以下のような構成を備える。即ち、少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムであって、前記ネットワーク介して接続され、前記ユーザ端末及びコンテンツサーバに対してディジタル識別情報を発行する認証装置と、前記ユーザ端末からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置と、前記コンテンツサーバ及び前記データ変換装置からの要求に応じて、前記コンテンツデータの配信及び前記コンテンツデータの変換に対応する課金を行う課金装置とを有し、前記ユーザ端末、前記データ変換装置及び前記課金装置は、前記認証装置からの前記ディジタル識別情報に基づく相互認証に成功した場合に送受信することを特徴とする。

【００１０】上記目的を達成するために本発明のデータ配信方法は以下のような工程を備える。即ち、少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムにおけるデータ配信方法であって、前記ネットワーク介して接続され、前記ユーザ端末及びコンテンツサーバに対してディジタル識別情報を発行する工程と、前記ユーザ端末からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置によりデータを変換する工程と、前記コンテンツサーバ及び前記データ変換装置からの要求に応じて、前記コンテンツデータの配信及び前記コンテンツデータの変換に対応する課金を課金装置により行わせる課金工程とを有し、前記ユーザ端末、前記データ変換装置及び前記課金装置は、前記ディジタル識別情報に基づく認証に成功した場合に送受信することを特徴とする。

【００１１】上記目的を達成するために本発明のデータ配信方法は以下のような工程を備える。即ち、少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムにおけるデータ配信方法であって、前記ユーザ端末及びコンテンツサーバからの要求に応じて、各対応するディジタル識別情報を発行する工程と、前記ユーザ端末から前記コンテンツサーバに対してコンテンツデータを要求する工程と、前記要求に応じて前記コンテンツサーバから、要求したユーザ端末に前記コンテンツデータを送信する送信工程と、前記コンテンツデータが前記ユーザ端末が処理可能な形式のデータでない場合に、当該ユーザ端末が処理可能なデータ形式のデータに変換するデータ変換工程と、前記コンテンツデータの配信及び前記コンテンツデータのデータ変換に対応する課金を行う課金工程とを有し、前記送信工程、前記データ変換工程及び前記課金工程は、前記ディジタル識別情報に基づく認証に成功した場合に実施されることを特徴とする。

【００１２】

【発明の実施の形態】以下、添付図面を参照して本発明の好適な実施の形態を詳細に説明する。

【００１３】まず最初に、一般的なＭＰＥＧ－４再生装置の構成と動作を説明する。

【００１４】図１は一般的なＭＰＥＧ－４再生装置（データ処理装置：ユーザ端末）の概略構成を示すブロック図である。

【００１５】図１において、伝送路１０１は各種ネットワーク、コンピュータバス等のデータの路であり、ＭＰＥＧ－４ストリームが入力されるネットワークである。ここで、伝送路１０１は通信路の意味の他にＣＤ－ＲＯＭ，ＤＶＤ－ＲＯＭ，ＤＶＤ－ＲＡＭといった記録媒体装置と再生装置とのインターフェースも意味する。

【００１６】この再生装置では、ネットワークから配信されたＭＰＥＧ－４データや、記録媒体装置から再生されたＭＰＥＧ－４データは分離部１０２に入力される。ここでＭＰＥＧ－４データは、シーン記述情報データ、動画像オブジェクトデータ、音声オブジェクトデータ、オブジェクト記述データ等に分離された後、それぞれのメモリ部１０３～１０６に入力される。

【００１７】ここで、音声オブジェクトデータは例えば、周知のＣＥＬＰ（Code Excited Linear Prediction）符号化や、変換領域重み付けインターリーブベクトル量子化（ＴＷＩＮＶＱ）符号化等の高効率符号化が施されたデータであり、動画像オブジェクトデータは、例えば、ＭＰＥＧ－４やＨ－２６３方式にて高効率符号化が施されたデータである。またオブジェクト記述データは、各オブジェクトに関する属性情報等を示すデータである。メモリ部１０４～１０６の各オブジェクトデータ

はそれぞれの復号部１０８～１１０へ入力され、復号部１０８～１１０において、上述のような高効率符号化された、動画像オブジェクトデータ、音声オブジェクトデータ、及びオブジェクト記述データ等が復号される。但し、メモリ部１０３に入力されたシーン記述情報データのみは、シーン記述復号部１０７へ直接入力されて復号される。

【００１８】尚、図１においては音声オブジェクト、動画像オブジェクト、オブジェクト記述データについて、それぞれ複数の互いに異なる種類のオブジェクトがＭＰＥＧ－４ストリームに内に存在しても復号可能な装置を仮定しているため、メモリ部１０４～１０６や復号部１０８～１１０は音声用、動画像用、オブジェクト記述データ用に夫々複数用意されているものとする。

【００１９】そして、復号部１０８～１１０においてそれぞれ復号された音声オブジェクト、動画像オブジェクト、オブジェクト記述データは、シーン記述復号部１０７で復号されたシーン記述情報データに基づいて、シーン合成部１１２にて合成／グラフィック処理が行われる。このようにして得られた最終的なデータ列はディスプレイやプリンタ装置といった出力機器１１３に供給されて可視化されることになる。

【００２０】ここで、音声或いは動画像などのシーンを構成する個々のオブジェクトデータに対して、著作権などの保護のために再生を実行させたり、再生を停止させたりする制御が必要となる場合には、ＩＰＭＰ(Intellectual Property Managementand Protection)情報を用いて制御を行う。このＩＰＭＰ情報は、受信データの構成要素であるＩＰＭＰデータにて伝送される。ＩＰＭＰ制御部１１１は、分離部１０２からのＩＰＭＰデータに含まれるＩＰＭＰ情報に基づき、必要に応じて制御ポイントにおいてストリームを遮断したり、復号部１０８～１１０にアクセスして、復号動作の停止を命令する。このためＩＰＭＰ制御部１１１が、ＩＰＭＰ情報等に基づいてデータの視聴の権利が無いと判断した場合には、該データが復号されなくなるので、再生が行われなくなる。このような制御を行うことで著作権を有するデータの保護を行う。

【００２１】このＩＰＭＰ情報は、図２に示すようなＩＰＭＰディスクリプタ、又はＩＰＭＰメッセージにて伝送されることになっている。しかし、図２からも分かるように、規格によって決められているのは、ＩＰＭＰ情報が記述されるべき領域のみであり、実際に使用されるデータのシンタックスについては何ら規定されていない。そのため、オブジェクトデータを提供する企業毎に異なるＩＰＭＰ情報が存在し、それらの間には互換性が無い可能性がある。このような場合には、自分のデータ処理装置が処理できるＩＰＭＰデータの型と、再生しようとするオブジェクトデータのＩＰＭＰデータの型とが一致していないと、所望するオブジェクトデータの再生が出来ないばかりか、場合によってはデータ処理装置が暴走する危険性もある。このような事態を回避するために以下のような方式が提案されている。

【００２２】この方式によると、ユーザが再生しようと所望するオブジェクトデータのＩＰＭＰデータの型を、ユーザ自身のデータ処理装置が処理できるＩＰＭＰデータの型に変換するデータ変換装置をデータ処理装置とオブジェクトデータの供給源（コンテンツサーバ）との間に置き、データの送受信は、このデータ変換装置を介して行うというものである。

【００２３】この仕組みを図３に基づいて説明する。コンテンツサーバ１(301)に格納してあるオブジェクトデータのＩＰＭＰデータの型は"１"であるとし、コンテンツサーバ２(302)に格納してあるオブジェクトデータのＩＰＭＰデータの型は"２"であるとする。一方、データ処理装置３０３が処理できるＩＰＭＰデータの型は"１"であるとする。このＩＰＭＰデータの型は、上記"１"，"２"の型の他にも複数存在することが考えられる。ここでは、データの型"１"から"２"への変換の場合について説明する。

【００２４】このデータ処理装置３０３がコンテンツサーバ１(301)のオブジェクトデータ（オブジェクトデータのＩＰＭＰデータの型は"１"）をネットワーク経由で受信した後に再生するのは、ＩＰＭＰデータの型が一致するので可能である。しかし、このデータ処理装置３０３がコンテンツサーバ２(302)のオブジェクトデータ（オブジェクトデータのＩＰＭＰデータの型は"２"）をネットワーク経由で受信して再生することは、ＩＰＭＰデータの型が一致しないため、不可能である。そこで、このような場合には、データ変換装置３０４においてコンテンツサーバ２(302)からのＩＰＭＰデータを変換してからデータ処理装置３０３に送信する。ここでは、ＩＰＭＰデータの型が"２"から"１"への変換が行われる。

【００２５】ここで著作権保護のために、オブジェクトデータに対してオブジェクトデータを提供する企業独自の暗号化をはじめとする様々なデータ変換が施されている場合は、それらのデータ変換の逆変換を行ってオリジナルの状態に戻してから、再度ユーザの持つデータ処理装置３０３が処理できるようなデータに変換する。このような処理を行うことで、ユーザの持つデータ処理装置３０３が処理できるＩＰＭＰデータの型がどうようなものでも、またユーザが再生を所望するオブジェクトデータのＩＰＭＰデータの型がどうようなものであっても、データを再生することが可能になる。

【００２６】次に本実施の形態に係るコンテンツサーバ１，２（３０１，３０２）、データ変換装置３０４、データ処理装置（ユーザ端末）３０３、証明書発行装置（認証装置）３０５を含むデータ配信システムにおける各装置間のデータの流れを説明する。

【００２７】図４は、本発明の実施の形態に係るデータ

配信システムにおける各装置間のデータの流れを説明する図である（課金装置無しのシステム）。

【００２８】ここで図３と同様に、データ処理装置３０３は、ＩＰＭＰデータの型が"１"のデータを処理及び表示することができ、コンテンツサーバ１(301)には、ＩＰＭＰデータの型が"１"のデータであるコンテンツデータ1が蓄積されており、コンテンツサーバ２(302)には、ＩＰＭＰデータの型が"２"のデータであるコンテンツデータ2が蓄積されている。データ変換装置３０４は、ＩＰＭＰデータの型が"１"のコンテンツデータ1をＩＰＭＰデータの型が"２"のデータ（コンテンツデータ1-ex2）に変換でき、その逆のＩＰＭＰデータの型が"２"のコンテンツデータ2をＩＰＭＰデータの型が"１"のデータ（コンテンツデータ2-ex1）に変換することもできる。更に、コンテンツデータ1に対して「方式１」により暗号化処理等のデータ変換が施されており、コンテンツデータ2に対して「方式２」により暗号化処理等のデータ変換が施されている場合に、これらの方式の変換、即ち、「方式１」による処理が施されているコンテンツデータ1を逆変換して元のオリジナルの状態に戻してから「方式２」によるデータ変換を施すといったデータ変換を行う。証明書発行装置３０５は、各装置からの証明書発行要求を受けると、その要求してきた装置に対して証明書を発行するかどうかを判断し、発行の許可を決定した装置に対して証明書を発行して送出する。

【００２９】以下、データ処理装置３０３が所望のコンテンツを得るまでの過程について記述する。

【００３０】予め各装置は、証明書発行装置３０５に証明書発行要求を送出して証明書を発行してもらいと、その証明書を自装置に保持しておく。データ処理装置３０３は、取得するコンテンツがユーザによって決められると、そのコンテンツが存在するコンテンツサーバに対して、そのサーバ内に複数存在するコンテンツから取得したいコンテンツを特定するために必要な番号を特定するコンテンツＩＤと、上記で得た証明書と、自分が処理できるＩＰＭＰの型を含むデータをリクエスト信号として送信する。ここでデータ処理装置３０３が処理できるＩＰＭＰデータの型は"１"であるとする。

【００３１】以下、各場合について説明する。

（１）：リクエスト信号を送信した先のコンテンツサーバが持つコンテンツデータのＩＰＭＰデータの型が"１"である場合（コンテンツサーバ１(301)の場合）

（１－１）：コンテンツサーバ１(301)は、証明書発行装置３０５から送られた証明書をチェックしてから、そのデータを要求しているデータ処理装置３０３が処理できるＩＰＭＰの型が"１"であることを確認する。このチェックは該証明書が改竄されていないか、有効期間内であるか、本当に証明書発行装置３０５によって発行されたものであるかどうか等について検証する。このチェック、ＩＰＭＰの型の確認が問題なく終了すると、次はコンテンツサーバ１(301)がデータ処理装置３０３に対して、自装置の証明書を含むデータを肯定応答信号として送信する。また、この証明書チェックにおいて、この証明書の不正が検出された場合には、否定応答信号をデータ処理装置３０３に対して送信する（図４の４０１で示す）。

【００３２】この否定応答信号を受信じたデータ処理装置３０３は、認証に失敗した旨のメッセージを表示して処理を終了する。

【００３３】一方、肯定応答信号を受信したデータ処理装置３０３は、送られてきたコンテンツサーバ１(301)の証明書をチェックし、該チェックが問題無く終了したら、今度はコンテンツＩＤで構成されるリクエスト信号をコンテンツサーバ１(301)に対して送る。コンテンツサーバ１(301)は、このリクエスト信号を受信すると、その要求されたコンテンツＩＤに対応するコンテンツデータを、そのデータ処理装置３０３に送信する（図の４０１）。このようにしてデータ処理装置３０３に送られたコンテンツデータに、ＩＰＭＰデータの型"１"に対応する暗号処理等のデータ変換処理を施すことにより、伝送路上等でデータが盗聴された場合でも、著作権を有するコンテンツデータの保護が実現できる。

【００３４】このコンテンツデータを受信したデータ処理装置３０３は、自装置に組み込まれているＩＰＭＰシステムを用いてＩＰＭＰデータの型が"１"のデータを処理して、ディスプレイやスピーカ等に出力する。また受信したコンテンツデータにＩＰＭＰデータの型"１"に対応する暗号処理等のデータ変換が施されている場合にも上記と同様に、自装置に組み込まれているＩＰＭＰシステムを用いて逆変換及びデータ処理を行いディスプレイやスピーカ等に出力する。

【００３５】次に、コンテンツデータに暗号処理がなされている場合の鍵データの流れについて説明する。

【００３６】このような暗号化処理が行われている場合、コンテンツサーバ１(301)からの鍵データはＩＰＭＰデータの中に含まれるか、或いは別途何らかのルートでデータ処理装置に送られる。

（２）：リクエスト信号を送信した先のコンテンツサーバが持つコンテンツデータのＩＰＭＰデータの型が"２"である場合（コンテンツサーバ２(302)の場合）

（２－１）：コンテンツサーバ２(302)は、送られた証明書をチェックしてから、データの要求をしているデータ処理装置３０３が処理できるＩＰＭＰの型を確認する。ここでは、データ処理装置３０３で処理できるＩＰＭＰの型が"１"であり、コンテンツサーバ２(302)の持つコンテンツデータのＩＰＭＰデータの型が"２"であるので、コンテンツサーバ２(302)は、データ処理装置３０３に対して、自装置の証明書を含むデータと、データ変換装置３０４のロケーション情報（ＩＰアドレス）を肯定応答信号として送信する（図４の４０２で示す）。

（２－２）：データ処理装置３０３は、この送られてきたコンテンツサーバ２(302)の証明書をチェックし、このチェックが問題無く終了したら、指定されたロケーション情報に基づき、データ変換装置３０４に対して所望するコンテンツＩＤと、該コンテンツＩＤのコンテンツが存在するコンテンツサーバのロケーション情報（ＩＰアドレス）と、自装置の証明書と、自分が処理できるＩＰＭＰの型とで構成されるデータをリクエスト信号として送信する（図４の４０３で示す）。

（２－３）：データ変換装置３０４は、この送られてきたデータ処理装置３０３の証明書をチェックし、このチェックが問題無く終了したら、自装置の証明書を含む肯定応答信号をデータ処理装置３０３に対して送る（図４の４０５で示す）と同時に、コンテンツサーバ２(302)に対してコンテンツＩＤと自装置の証明書とで構成されるデータをリクエスト信号として送信する（図４の４０４で示す）。

【００３７】一方、データ変換装置３０４は、このチェックにおいて不正が検出された場合には、否定応答信号をデータ処理装置３０３に対して送信する（４０５）。この否定応答信号を受信したデータ処理装置３０３は、認証に失敗した旨のメッセージを表示して処理を終了する。

【００３８】また、（２－３）で送信されたデータ変換装置３０４の証明書を含む肯定応答信号を受信したデータ処理装置３０３は、この証明書のチェックを行う。このチェックにおいて不正が検出された場合には、認証に失敗した旨のメッセージを表示して処理を終了する。

【００３９】コンテンツサーバ２(302)は、出た変換装置３０４から受信したリクエスト信号に含まれるデータ変換装置３０４の証明書をチェックしてから、その要求されたコンテンツＩＤに対応するコンテンツデータ2をデータ変換装置３０４に送信する（４０４）。

【００４０】一方、コンテンツサーバ２(302)における証明書のチェックにおいて不正が検出された場合には、否定応答信号をデータ変換装置３０４に対して送信する（４０４）。この否定応答信号を受信したデータ変換装置３０４は、データ処理装置３０３に対して否定応答信号を送信する（４０５）。

【００４１】ここで、データ変換装置３０４がコンテンツサーバ２(302)から受信したコンテンツデータ2のＩＰＭＰデータの型は"２"であり、この実施の形態に係るデータ処理装置３０３が処理可能なデータの型ではない。従って、このコンテンツデータ2を受信したデータ変換装置３０４は、このデータ処理装置３０３が処理できるようにコンテンツデータ2をデータ変換する。

【００４２】具体的には、コンテンツデータ2のＩＰＭＰデータの型は"２"であるので、該ＩＰＭＰデータの型を"２"から"１"に変換する処理を行う。ここで、コンテンツデータ2にＩＰＭＰデータの型"２"に対応する暗号処理等のデータ変換が施されている場合には、この変換の逆変換を行うことでコンテンツデータを一旦元の状態に戻し、今度はＩＰＭＰデータの型"１"に対応する暗号処理等のデータ変換を行う。これらの処理によりコンテンツデータ2は、データ処理装置３０３で処理できるコンテンツデータ(2-ex1)に変換される。

（２－４）：データ変換装置３０４は、このコンテンツデータ(2-ex1)をデータ処理装置３０３に送信する（図４の４０５）。このコンテンツデータ(2-ex1)を受信したデータ処理装置３０３は、自装置に組み込まれているＩＰＭＰシステムを用いて上記データを処理して、ディスプレイやスピーカ等に出力する。

【００４３】また、受信したコンテンツデータにＩＰＭＰデータの型"１"に対応する暗号処理等のデータ変換が施されている場合も、自装置に組み込まれているＩＰＭＰシステムを用いて逆変換及びデータ処理を行ってディスプレイやスピーカ等に出力する。

【００４４】ここで、コンテンツデータに暗号処理がなされている場合の鍵データの流れについて説明する。

【００４５】このような暗号化処理が行われている場合、コンテンツサーバ２(302)からの鍵データは、ＩＰＭＰデータの中に含まれる形でデータ変換装置３０４に送信された後に、データ変換装置３０４にてデータ処理装置３０３が処理を行えるＩＰＭＰデータの型に変換されてからデータ処理装置３０３に送られるか、又は別途何らかのルートでデータ処理装置３０３に送られる。

【００４６】図５は、本発明の実施の形態に係る配信システムにおける各装置間のデータの流れを示す図である（課金装置５０１有りの場合のシステム）。

【００４７】データ処理装置３０３は、ＩＰＭＰデータの型が"１"のデータを処理及び表示することができ、コンテンツサーバ１(301)には、ＩＰＭＰデータの型が"１"のデータであるコンテンツデータ1が蓄積されており、コンテンツサーバ２(302)には、ＩＰＭＰデータの型が"２"のデータであるコンテンツデータ2が蓄積されている。データ変換装置３０４は、ＩＰＭＰデータの型が"１"のコンテンツデータ1を、ＩＰＭＰデータの型が"２"のデータ（コンテンツデータ(1-ex2)に変換でき、その逆のＩＰＭＰデータの型が"２"のコンテンツデータ2を、ＩＰＭＰデータの型が"１"のデータ（コンテンツデータ(2-ex1)に変換することもできる。更に、コンテンツデータ1に対して「方式１」により暗号化処理等のデータ変換が施されており、またコンテンツデータ2に対して「方式２」により暗号化処理等のデータ変換が施されている場合に、これらの方式の間の変換、即ち、「方式１」による処理が施されているコンテンツデータ1を逆変換して元のオリジナルの状態に戻してから「方式２」によるデータ変換を施すといったデータ変換を行う。

【００４８】課金装置５０１は、データ変換装置３０４

又はコンテンツサーバ１(301)から、このサーバ１やデータ変換装置３０４がデータ処理装置３０３に送付したコンテンツデータの対価に関するデータ（課金／決済を行うために必要となるデータ）を受け取り、ユーザ毎の課金データを生成する。この課金装置５０１は、外部の金融機関等と接続されており、この課金装置５０１で生成した課金データがこれらの機関に送られる。証明書発行装置３０５は、各装置からの証明書発行要求を受けると、その要求してきた装置に対して証明書を発行するかどうかを判断し、発行の許可を決定した装置に対しては証明書を発行／送出する。

【００４９】以下、データ処理装置３０３が所望のコンテンツを得るまでの過程について記述する。

【００５０】予め各装置は、証明書発行装置３０５に証明書発行要求を送出し、証明書を発行してもらい自装置に保持しておく。データ処理装置３０３は、取得するコンテンツがユーザによって決められると、そのコンテンツが存在するコンテンツサーバに対して、そのコンテンツサーバ内に複数存在するコンテンツから取得したいコンテンツデータを特定するために必要な番号であるコンテンツＩＤと、上記で得た証明書と、自分が処理できるＩＰＭＰの型とで構成されるデータをリクエスト信号として送信する。ここでデータ処理装置３０３が処理できるＩＰＭＰデータの型は"１"であるとする。

（１）：リクエスト信号を送信した先のコンテンツサーバが持つコンテンツデータのＩＰＭＰデータの型が"１"である場合（コンテンツサーバ１(301)の場合）

（１－１）：コンテンツサーバ１(301)は、送られた証明書をチェックしてから、そのコンテンツデータを要求しているデータ処理装置３０３が処理できるＩＰＭＰの型が"１"であることを確認する。このチェックは該証明書が改竄されていないか、有効期間内であるか、本当に証明書発行装置３０５によって発行されたものであるかどうか等について検証する。このチェック、ＩＰＭＰの型の確認が問題無く終了すると、次にコンテンツサーバ１(301)は、そのデータ処理装置３０３に対して、自装置の証明書を含むデータを肯定応答信号として送信する（図５の５０１）。尚、この証明書チェックにおいて。この証明書の不正が検出された場合には、否定応答信号をデータ処理装置３０３に対して送信する。

【００５１】コンテンツサーバ１(301)から肯定応答信号を受信したデータ処理装置３０３は、上記と同様に、送られてきたコンテンツサーバ１(301)の証明書をチェックし、このチェックが問題無く終了したら、今度はコンテンツＩＤで構成されるリクエスト信号をコンテンツサーバ１(301)に対して送る。コンテンツサーバ１(301)は、このリクエスト信号を受信すると、要求されたコンテンツＩＤに対応するデータをデータ処理装置３０３に送信すると同時に、課金／決済を行うために必要となるデータを生成する。

【００５２】一方、否定応答信号を受信したデータ処理装置３０３は、認証に失敗した旨のメッセージを表示して処理を終了する。

【００５３】コンテンツサーバ１(301)において生成される課金／決済を行うために必要となるデータの構成例を図６に示す。

【００５４】このデータはユーザ名、ユーザＩＤ、送信したコンテンツＩＤ、送信した日時等で構成される。

（１－２）：このデータが課金装置５０１に送られて（図５の５０２）、そこで課金データが生成される。

【００５５】ここでデータ処理装置３０３に送られたコンテンツデータに、ＩＰＭＰデータの型"１"に対応する暗号処理等のデータ変換を施すことにより、伝送路上等でデータが盗聴された場合でも著作権を有するコンテンツデータの保護が実現できる。このコンテンツデータを受信したデータ処理装置３０３は、自装置に組み込まれているＩＰＭＰシステムを用いてＩＰＭＰデータの型が"１"のデータを処理し、ディスプレイやスピーカ等に出力する。

【００５６】また、受信したコンテンツデータにＩＰＭＰデータの型"１"に対応する暗号処理等のデータ変換が施されている場合にも上記と同様に、自装置に組み込まれているＩＰＭＰシステムを用いて、逆変換及びデータ処理を行ってディスプレイやスピーカ等に出力する。

【００５７】ここで、コンテンツデータに暗号処理がなされている場合の鍵データの流れについて説明する。

【００５８】このような暗号化処理が行われている場合、コンテンツサーバ１(301)からの鍵データはＩＰＭＰデータの中に含まれるか、或いは別途何らかのルートでデータ処理装置３０３に送られる。この際、コンテンツサーバ１(301)は、鍵データを送信した記録として、図６の「鍵データの送信」欄に鍵データを格納する。このコンテンツデータに暗号化等のデータ変換が施されていない場合には、このコンテンツデータは無料と考えて課金の対象にしない。一方、暗号化等のデータ変換が施されている場合には、このコンテンツデータを有料と考えて課金を行うといったことが考えられる。このような場合には、この鍵データの存在するブロックのみを課金／決済を行うために必要となるデータとすることができる。

（２）：リクエスト信号を送信した先のコンテンツサーバが持つコンテンツデータのＩＰＭＰデータの型が"２"である場合（コンテンツサーバ２(302)の場合）

（２－１）：コンテンツサーバ２(302)は、送られた証明書をチェックしてから、データを要求をしているデータ処理装置３０３が処理できるＩＰＭＰの型を確認する。ここでは、データ処理装置３０３で処理できるＩＰＭＰの型が"１"であり、コンテンツサーバ２(302)の持つコンテンツデータのＩＰＭＰデータの型が"２"であるので、コンテンツサーバ２(302)は、データ処理装置３

０３に対して、自装置の証明書を含むデータと、データ変換装置３０４のロケーション情報（ＩＰアドレス）を肯定応答信号として送信する（図５の５０３）。

（２－２）：データ処理装置３０３は、送られてきたコンテンツサーバ２(302)の証明書をチェックし、このチェックが問題無く終了したら、指定されたロケーション情報に基づいて、データ変換装置３０４に対して所望するコンテンツＩＤと、そのコンテンツＩＤのコンテンツが存在するコンテンツサーバのロケーション情報（ＩＰアドレス）と、自装置の証明書と、自分が処理できるＩＰＭＰの型とで構成されるデータを、リクエスト信号としてデータ変換装置３０４に送信する（図５の５０４）。

（２－３）：データ変換装置３０４は、その送られてきたデータ処理装置３０３の証明書をチェックし、該チェックが問題無く終了したら、自装置の証明書を含む肯定応答信号をデータ処理装置３０３に対して送ると（５０５）同時に、コンテンツサーバ２(302)に対して、コンテンツＩＤと自装置の証明書とで構成されるデータをリクエスト信号として送信する（５０６）。コンテンツサーバ２(302)は、その受信したデータ変換装置３０４の証明書をチェックしてから、リクエスト信号で要求されたコンテンツＩＤに対応するコンテンツデータ2をデータ変換装置３０４に送信する（５０６）。そして、これと同時に、課金を行うために必要となるデータを生成する。このデータは上記図６と同様のデータである。ここで、データ変換装置３０４がコンテンツサーバ２(302)から受信したコンテンツデータ2のＩＰＭＰデータの型は"２"であり、このコンテンツデータ2を受信したデータ変換装置３０４は、データ処理装置３０３がコンテンツデータ2を処理可能になるようにデータの変換を行う。

【００５９】一方、データ変換装置３０４における上記証明書をチェックで不正が検出された場合には、否定応答信号をデータ処理装置３０３に対して送信する（５０５）。この否定応答信号を受信したデータ処理装置３０３は、認証に失敗した旨のメッセージを表示して処理を終了する。

【００６０】またデータ変換装置３０４から、証明書を含む肯定応答信号を受信したデータ処理装置３０３は、該証明書のチェックを行う。このチェックにおいて不正が検出された場合には、その認証に失敗した旨のメッセージを表示して処理を終了する。

【００６１】また一方、このチェックにおいて不正が検出された場合には、否定応答信号をデータ変換装置３０４に対して送信する。この否定応答信号を受信したデータ変換装置３０４は、データ処理装置３０３に対して否定応答信号を送信する。

【００６２】チェックが問題ない場合には、データ変換装置３０４は、コンテンツデータ2のＩＰＭＰデータの型が"２"であるので、このＩＰＭＰデータの型を"２"から"１"に変換する処理を行う。ここで、コンテンツデータ2にＩＰＭＰデータの型"２"に対応する暗号処理等のデータ変換が施されている場合には、該変換の逆変換を行うことでコンテンツデータを元の状態に戻し、その後、ＩＰＭＰデータの型"１"に対応する暗号処理等のデータ変換を行う。これらの処理によりコンテンツデータ2は、データ処理装置３０３が処理できるコンテンツデータ(2-ex1)に変換される。

（２－４）：課金を行うために必要となるデータが、コンテンツサーバ２(302)から課金装置５０１に送られ課金データが生成される（図５の５０８）。

（２－５）：データ変換装置３０４は、変換したコンテンツデータ(2-ex1)をデータ処理装置３０３に送信する（５０５）。更に、データ変換を行ったことに対する料金を計算するためのデータを生成する。

【００６３】このデータの構成例を図７に示す。

【００６４】このデータは、ユーザ名、ユーザＩＤ、変換したコンテンツＩＤ（送信コンテンツＩＤ）、送信した日時、変換したデータ量、どんな型のＩＰＭＰデータに変換したかを示す情報等で構成される。

（２－６）：このデータがデータ変換装置３０４から課金装置５０１に送られて課金データが生成される（５０７）。

【００６５】又、データ変換装置３０４からコンテンツデータ(2-ex1)を受信したデータ処理装置３０３は、自装置に組み込まれているＩＰＭＰシステムを用いて上記データを処理し、ディスプレイやスピーカ等に出力する。また、受信したコンテンツデータにＩＰＭＰデータの型"１"に対応する暗号処理等のデータ変換が施されている場合にも、自装置に組み込まれているＩＰＭＰシステムを用いて逆変換及びデータ処理を行ってディスプレイやスピーカ等に出力する。

【００６６】次に、コンテンツデータに暗号処理がなされている場合の鍵データの流れについて説明する。

【００６７】このような暗号化処理が行われている場合、コンテンツサーバ２(302)からの鍵データは、ＩＰＭＰデータの中に含まれる形でデータ変換装置３０４に送信された後、このデータ変換装置３０４において、データ処理装置３０３が処理を行えるようなＩＰＭＰデータの型に変換されてからデータ処理装置３０３に送られるか、または別途何らかのルートでデータ処理装置３０３に送られる。データ変換装置３０３を経由して鍵データが送られた場合、上述の場合と同様に、データ変換装置３０４は、鍵データを送信した記録として図７の「鍵データの送信」欄に鍵データを格納する。

【００６８】ここでは、図４および図５に基づいて各装置間のデータの流れについて説明したが、このデータの流れは一つの例であり、他にも様々なデータの流れが存在する。しかし他のデータの流れにおいても、データ処

理装置３０３が処理できないＩＰＭＰデータを持つコンテンツデータを要求した場合には、そのコンテンツデータはデータ変換装置３０４を経由して、要求元であるデータ処理装置３０３に入力されて、データ処理及び表示が行われる。また課金を行うために必要なデータが、データ変換装置３０４やコンテンツサーバから課金装置５０１に入力されるという点は、上記実施の形態と同様である。

【００６９】以下、本実施の形態に係る各装置の動作、特にデータ処理装置３０３の処理の一例について図８のフローチャートを用いて説明する。

【００７０】図８は、本実施の形態に係る配信システムにおいて、データ処理装置３０３がデータ変換装置３０４、コンテンツサーバからのデータを受信し、そのデータを再生する際の処理を説明するためのフローチャートである。

【００７１】図８において、まずステップＳ８０１で、証明書発行装置３０５に証明書発行要求を送出して証明書を発行／送信してもらい、その証明書を自装置に保持する。以後の認証処理では、この保持している証明書を用いて認証が行われる。

【００７２】次にステップＳ８０２に進み、このデータ処理装置３０３のユーザにより、再生したいコンテンツが決定されると、そのコンテンツを取得するために必要な情報がデータ処理装置３０３に入力される。これによりステップＳ８０３で、データ処理装置３０３から、コンテンツサーバに対して、そのサーバ内に複数存在するコンテンツから所望のコンテンツを特定するために必要な番号であるコンテンツＩＤと、証明書発行装置３０５からの証明書と、自装置が処理できるＩＰＭＰの型とで構成されるデータをリクエスト信号として送信する。

【００７３】次にステップＳ８０４に進み、そのコンテンツサーバからの応答が肯定応答信号であるか、否定応答信号であるかを判断する。応答が否定応答信号である場合はステップＳ８０５に進む。ここで、受信した応答が否定応答信号であるということは、自装置の証明書が接続先のコンテンツサーバにおいて認証されなかったことを意味するので、「証明書がコンテンツサーバにて認証されませんでした」とのメッセージを表示部（不図示）に表示して処理を終了する。

【００７４】一方ステップＳ８０４で、応答が肯定応答信号である場合はステップＳ８０６に進み、コンテンツサーバの証明書のチェックを行う。このチェックは、その証明書が改竄されていないか、有効期間内であるか、又、本当に証明書発行装置３０５によって発行されたものであるかどうか等について検証するものである。この検証の結果、証明書が正当でないと判断した場合にはステップＳ８０７に進み、コンテンツサーバの証明書を認証できなかったことを意味する「コンテンツサーバの証明書を認証することが出来ませんでした」とのメッセージを表示して処理を終了する。

【００７５】一方ステップＳ８０６で、チェックにより証明書が正当であると判断した場合はステップＳ８０８に進み、肯定応答信号の中のロケーション情報（データ変換装置３０４のＩＰアドレス等）があるか無いかが検証される。ここで、ロケーション情報があるということは、接続先のコンテンツサーバの持つコンテンツデータのＩＰＭＰデータの型が自装置では処理出来ないことを意味し、ロケーション情報が無いということは、接続先のコンテンツサーバの持つコンテンツデータのＩＰＭＰデータの型が自装置で処理出来ることを意味する。従って、ロケーション情報が無い場合はステップＳ８０９に進み、コンテンツＩＤで構成されるリクエスト信号をコンテンツサーバに対して送る。次にステップＳ８１０に進み、所望するコンテンツデータを受信して、自装置に組み込まれているＩＰＭＰシステムを用いて、そのコンテンツデータを処理し、ディスプレイやスピーカ等に出力して処理を終了する。

【００７６】一方、ステップＳ８０８で、ロケーション情報が有る場合、即ち、接続先のコンテンツサーバの持つコンテンツデータのＩＰＭＰデータの型が自装置では処理出来ない場合にはステップＳ８１１に進み、そのロケーション情報に基づき、所望するコンテンツＩＤと、そのコンテンツＩＤのコンテンツの存在するコンテンツサーバのロケーション情報（ＩＰアドレス）と、自装置の証明書と、自分が処理できるＩＰＭＰの型とで構成されるデータを、データ変換装置３０４に対してリクエスト信号として送信する。次にステップＳ８１２に進み、データ変換装置３０４からの応答が肯定応答信号か、否定応答信号であるかを判断する。応答が否定応答信号である場合にはステップＳ８１３に進む。ここで、受信した応答が否定応答信号であるということは、自装置の証明書が接続先のデータ変換装置３０４において認証されなかったか、又はコンテンツサーバにおいてデータ変換装置３０４の証明書が認証されなかったことを意味するので、「証明書が認証されませんでした」とのメッセージを表示して処理を終了する。

【００７７】一方、ステップＳ８１２で、応答が肯定応答信号である場合にはステップＳ８１４に進み、データ変換装置３０４の証明書のチェックを行う。このチェックは、その証明書が改竄されていないか、有効期間内であるか、また本当に証明書発行装置３０５によって発行されたものであるかどうか等について検証するものである。この検証の結果、その証明書が正当でないと判断した場合にはステップＳ８１５に進み、データ変換装置３０４の証明書を認証できなかったことを意味する「データ変換装置の証明書を認証することが出来ませんでした」とのメッセージを表示して処理を終了する。

【００７８】またステップＳ８１４で、データ変換装置３０４の証明書のチェックにより正当であると判断した

場合にはステップＳ８１６に進み、要求しているコンテンツデータを受信して、自装置に組み込まれているＩＰＭＰシステムを用いて、そのコンテンツデータを処理し、ディスプレイやスピーカ等に出力して処理を終了する。

【００７９】次に、上記の認証処理で用いられる証明書の発行処理を行う証明書発行装置３０５の処理の一例について図９のフローチャートを用いて説明する。

【００８０】図９は、証明書発行装置３０５がデータ処理装置３０３、データ変換装置３０４、コンテンツサーバ３０１、３０２、課金装置５０１からの証明書発行要求を受信し、各証明書の発行を行う際の処理を説明するためのフローチャートである。

【００８１】図９において、まずステップＳ９０１で、データ処理装置３０３、データ変換装置３０４、コンテンツサーバ３０１，３０２、課金装置５０１から証明書発行要求をネットワーク経由で受信する。この証明書発行要求は、要求者の識別名、自装置に関する公開情報、これらのデータが伝送路上で改竄されていないことを証明するためのデータ等で構成される。

【００８２】この要求を受信するとステップＳ９０２に進み、各装置から受信した証明書発行要求を解析する。具体的には、データの改竄を証明するデータを用いて、要求者の識別名や自装置に関する公開情報等が改竄されていないかどうか、証明書を登録してあるデータベースに既に登録されていないかどうか、一度発行した証明書を無効にするためのデータベースに登録されていないかどうか、場合によっては識別名が示す組織、会社が実際に存在するかどうかといったことに関する各種チェックを行う。ここで、この証明書発行に際して、そのチェックを厳格に行うか、或いは簡易に行うのかを設定できるような仕組みが備わっていることが望ましい。

【００８３】この解析が終了するとステップＳ９０３に進み、ステップＳ９０２における解析結果に基づいて、各装置に対する証明書を発行するかどうかを判断する。ここで発行を行わないと判断した場合にステップＳ９０７に進み、証明書が発行できなかったこと旨のメッセージを証明書発行要求を送信してきた発行元の装置に送信して、処理を終了する。

【００８４】一方ステップＳ９０３で、発行を行うと判断した場合にはステップＳ９０４に進み、その証明書発行要求の内容に基づいて発行処理を行う。ここで発行される証明書は、証明書のバージョン番号、シリアル番号、証明書を発行した装置名、有効期限、ユーザの公開情報、該証明書が伝送路上で改竄されていないことを証明するためのデータ等で構成される。次にステップＳ９０５に進み、ステップＳ９０４で発行した証明書を、その証明書発行要求を送信してきた各装置に送信する。次にステップＳ９０６に進み、上記ステップＳ９０４で発行した証明書を登録用データベースに登録し、同じ識別名で２重の登録がなされないように管理する。なお、この登録用データベースは、証明書発行装置３０５の内部に設けられていても良く、或いは証明書発行装置３０５の外部にあって、ネットワーク等で接続された装置内に設けられていても良い。こうしてステップＳ９０６の登録処理が済めば処理終了となる。

【００８５】尚、ここで、一度発行された証明書を何らかの理由により無効にしたい場合は、その証明書を所有している装置は証明書発行装置３０５に対して、証明書無効化要求を送信する。これにより証明書発行装置３０５は、無効となる証明書のみを含む無効データベースに、その要求された証明書を移動して登録する。このような処理を行うことで、その要求された証明書を無効とすることができる。

【００８６】次に、コンテンツの対価に対する決済を行う課金装置５０１の処理の一例について図１０のフローチャートを用いて説明する。

【００８７】図１０は、課金装置５０１がデータ変換装置３０３、コンテンツサーバ３０１，３０２からの課金／決済を行うためのデータを受信し、その受信したデータに基づいて行う決済処理を説明するためのフローチャートである。

【００８８】図１０において、まずステップＳ９０１で、データ変換装置３０４、コンテンツサーバ３０１，３０２から課金／決済を行うためのデータを受信する。このデータは前述の図６や図７で示されるものである。次にステップＳ１００２み進み、ステップＳ１００１で受信したデータを基にしてユーザ毎の課金データを生成する。次にステップＳ１００３に進み、ステップＳ１００２で生成した課金データをデータベースに登録して、ユーザ毎に管理する。なお、このデータベースは課金装置５０１の内部に存在してもよいし、この課金装置５０１の外部にあるネットワーク等で接続された装置に存在してもよい。

【００８９】次にステップＳ１００４に進み、課金データの送信時間であるかどうかが判断される。これは例えば、金融機関は月末等の一定期間毎に決済処理を行っている。そのため、この課金データは生成される毎に送信する必要は必ずしも無い。そこである一定期間を予め決めておき、その時間が来たら一気に課金データを送信するようにする。ステップＳ１００４で送信時間になった時はステップＳ１００５に進み、そうでない時は送信時間がくるまで、このステップＳ１００４を繰り返す。

【００９０】ステップＳ１００５では、ステップＳ１００３で登録した課金データを、スケジュールに従って、対応する銀行やクレジット会社等の金融機関の処理装置に送信する。次にステップＳ１００６に進み、送信した課金データに対する応答が肯定応答信号であるかどうかが判断される。金融機関の処理装置は、課金データを確実に受信した場合には肯定応答信号を課金装置５０１に

対して送信し、一方、受信に失敗した場合には否定応答信号を送信するので、応答が肯定応答信号である場合には、課金装置５０１は、課金データが正常に受信されたと判断して処理を終了する。

【００９１】一方、応答が否定応答信号である場合には、前回ステップＳ１００５で送信した課金データが受信されていないと判断して再度ステップＳ１００５に戻り、ステップＳ１００６で肯定応答信号を受取るまで、このステップＳ１００５の処理を繰り返す。

【００９２】次に、コンテンツデータの変換を行うデータ変換装置３０４の処理の一例について図１１のフローチャートを用いて説明する。

【００９３】図１１は、データ変換装置３０４がコンテンツサーバからのコンテンツデータを受信し、そのコンテンツデータをデータ処理装置３０３が処理できるようなデータに変換するための処理を説明するためのフローチャートである。なお、このデータ変換装置３０４が動作するのは、データ処理装置３０３が処理可能なＩＰＭＰデータの型とユーザが所望するコンテンツデータのＩＰＭＰデータの型とが異なる場合である。

【００９４】図１１において、まずステップＳ１１０１で、データ処理装置３０３が変換を所望するコンテンツＩＤと、そのコンテンツＩＤのコンテンツが存在するコンテンツサーバのロケーション情報（ＩＰアドレス）と、データ処理装置３０３の証明書と、データ処理装置３０３が処理できるＩＰＭＰの型とを含むデータを、リクエスト信号としてデータ処理装置３０３から受信する。このリクエスト信号を受信するとステップＳ１１０２に進み、ステップＳ１１０１で受信したデータ処理装置３０３の証明書のチェックを行う。このチェックは、データ処理装置３０３の証明書が改竄されていないか、有効期間内であるか、また本当に証明書発行装置３０５によって発行されたものであるかどうか等について検証するものである。この検証の結果、その証明書が正当でないと判断した場合にはステップＳ１１０３に進み、証明書の検証に失敗したので、データ処理装置３０３に対して否定応答信号を送信して処理を終了する。

【００９５】ステップＳ１１０２で、正当であると判断した場合はステップＳ１１０４に進み、上記ローケーション情報（ＩＰアドレス）で示されているコンテンツサーバに対してコンテンツＩＤとデータ変換装置３０４の証明書とを含むリクエスト信号を送信する。これと同時に、その要求元のデータ処理装置３０３に対して、そのデータ変換装置３０４の証明書を含む肯定応答信号を送信する。

【００９６】次にステップＳ１１０５に進み、コンテンツサーバから受信したデータがコンテンツデータであるか、否定応答信号であるのかを判断する。ここで、受信したデータが否定応答信号である場合にはステップＳ１１０６に進む。ここでは、コンテンツサーバにおいてデータ変換装置３０４の証明書が認証されなかったために否定応答信号を受信したのであるため、データ処理装置３０３に否定応答信号を送信して処理を終了する。

【００９７】一方、ステップＳ１１０５で、コンテンツサーバから受信したデータがコンテンツデータである場合はステップＳ１１０７に進み、ステップＳ１１０５で受信したコンテンツデータを、ステップＳ１１０１でリクエスト信号を送信してきたデータ処理装置３０３が処理できるようなデータに変換する。次にステップＳ１１０８に進み、ステップＳ１１０７で変換したコンテンツデータを、そのデータ変換を要求してきたデータ処理装置３０３に送信する。そしてステップＳ１１０９に進み、データ変換を行ったことに対する料金を計算するために必要となるデータを生成する。このデータは図７に示されるものである。そして、生成したデータを課金装置５０１に対して送信して処理を終了する。

【００９８】次に、コンテンツデータが格納されているコンテンツサーバの処理の一例について図１２のフローチャートを用いて説明する。

【００９９】図１２は、本実施の形態に係るコンテンツサーバの行う処理を説明するためのフローチャートである。

【０１００】図１２において、まずステップＳ１２０１で、ユーザが取得したいコンテンツを特定するために必要な番号であるコンテンツＩＤと、データ処理装置３０３の証明書と、データ処理装置３０３が処理できるＩＰＭＰの型とを含むデータを、リクエスト信号としてデータ処理装置３０３から受信する。このリクエスト信号を受信するとステップＳ１２０２に進み、ステップＳ１２０１で受信したデータ処理装置３０３の証明書のチェックを行う。このチェックは、その証明書が改竄されていないか、有効期間内であるか、また本当に証明書発行装置３０５によって発行されたものであるかどうか等について検証するものである。この検証の結果、証明書が正当でないと判断した場合にはステップＳ１２０３に進む。この場合は、リクエスト信号を発行したデータ処理装置３０３の証明書の検証に失敗したので、そのデータ処理装置３０３に対して否定応答信号を送信して処理を終了する。

【０１０１】一方、ステップＳ１２０２で、その証明書が正当であると判断した場合にはステップＳ１２０４に進み、ステップＳ１２０１で受信したリクエスト信号の発行元であるデータ処理装置３０３が処理できるＩＰＭＰの型と、コンテンツサーバ内にあるコンテンツデータのＩＰＭＰデータの型とが一致するかどうかを判断する。一致していると判断された場合はステップＳ１２０５に進み、そのデータ処理装置３０３に対して、コンテンツサーバの証明書を含むデータを肯定応答信号として送信する。次にステップＳ１２０６に進み、データ処理装置３０３からコンテンツＩＤで構成されるリクエスト

信号を受信する。そしてステップＳ１２０７に進み、ステップＳ１２０６で受信したリクエスト信号により要求されたコンテンツＩＤに対応するデータをデータ処理装置３０３に送信する。これと同時に、コンテンツデータに対する課金を行うために必要となるデータを生成する。この生成したデータは図６に示されるものである。そしてステップＳ１２０８に進み、ステップＳ１２０７で生成したコンテンツデータに対する課金を行うために必要となるデータを課金装置３０５に送信して処理を終了する。

【０１０２】一方、ステップＳ１２０４で、ＩＰＭＰの型が不一致と判断した場合にはステップＳ１２０９に進み、そのデータ処理装置３０３に対して、コンテンツサーバの証明書を含むデータとデータ変換装置３０４のロケーション情報（ＩＰアドレス）とを含むデータを肯定応答信号として送信する。次にステップＳ１２１０に進み、コンテンツＩＤとデータ変換装置３０４の証明書とを含むデータをリクエスト信号として、そのデータ処理装置３０３から受信する。これによりステップＳ１２１１に進み、ステップＳ１２１０で受信したデータ変換装置３０４の証明書のチェックを行う。このチェックは、その証明書が改竄されていないか、有効期間内であるか、また本当に証明書発行装置３０５によって発行されたものであるかどうか等について検証するものである。この検証の結果、証明書が正当でないと判断した場合にはステップＳ１２１２に進み、データ変換装置３０４に対して否定応答信号を送信して処理を終了する。

【０１０３】一方、ステップＳ１２１１で、正当であると判断した場合にはステップＳ１２１３に進み、ステップＳ１２１０で要求されたコンテンツＩＤに対応するコンテンツデータをデータ変換装置３０４に送信する。これと同時に、コンテンツデータに対する課金を行うために必要となるデータを生成するこの該データは図６に示されるものである。次にステップＳ１２１４に進み、ステップＳ１２１３で生成したコンテンツデータに対する課金を行うために必要となるデータを課金装置３０５に送信して処理を終了する。

【０１０４】以上説明したように本実施の形態によれば、ユーザが使用するデータ処理装置からコンテンツサーバに対してコンテンツを要求して、そのコンテンツをユーザが取得できるとともに、そのコンテンツが自装置で処理できないデータの場合には、データ変換装置を使用してデータ変換を行い、その変換されたデータを受取ることにより、自装置の有していない方式で暗号化されたデータでも受信して再生できる。

【０１０５】更に、この構成に、証明書発行装置から発行された証明書による認証機能を付加することにより、認証された装置間でのデータの交換を行うことができる。

【０１０６】更に本実施の形態に係る特徴的な構成として、コンテンツサーバ、データ変換装置は、ユーザからの要求に応じてコンテンツの提供、データ変換を実行すると、課金装置５０１により、それに伴う課金データを生成して、データ変換装置３０３、コンテンツサーバ３０１，３０２からの課金／決済を行うことができる。これによりそのコンテンツの著作権者は、そのコンテンツの視聴を許可している人にだけそのコンテンツを提供でき、かつそのコンテンツを提供することによる報酬（課金）を自動的に得られるので、安心してコンテンツを提供することができる。

【０１０７】本発明は一つの機器（例えば複写機、ファクシミリ）からなる装置に適用しても、複数の機器（例えばホストコンピュータ、インタフェース機器、リーダ、プリンタ等）から構成されるシステムに適用してもよい。

【０１０８】また、前述した実施形態の機能を実現する様に各種のデバイスを動作させるために、該各種デバイスと接続された装置あるいはシステム内のコンピュータに、前記、実施形態を実現するためのソフトウェアのプログラムを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵ，ＭＰＵ）を格納させたプログラムに従って前記各種デバイスを動作させることによって実施したものも本発明の範疇に含まれる。

【０１０９】またこの場合、前記ソフトウェアのプログラム自体が前述した実施形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばプログラムコードを格納した記憶媒体は本発明を構成する。

【０１１０】かかるプログラムコードを格納する記憶媒体としては例えばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、不揮発性のメモリカード等を用いることができる。

【０１１１】またコンピュータが、供給されたプログラムコードを実行することにより、前述の実施形態の機能が実現されるだけではなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）、あるいは他のアプリケーションソフト等と共同して前述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【０１１２】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその拡張機能ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も本発明の実施の形態に含まれることは言うまでもない。

【０１１３】以上説明したように本実施の形態によれ

ば、データ変換システム及びＩＰＭＰシステムと連携したユーザ認証、課金システムが構築できる。その結果、ネットワークを使用したコンテンツ配信サービスが現実的なものとなる。

【０１１４】

【発明の効果】以上説明したように本発明によれば、ユーザの認証に加えて、そのユーザによるコンテンツデータの取得及びデータ変換に伴う課金を自動的に行うことができる。

【０１１５】又本発明によれば、視聴を許可されたユーザだけがそのコンテンツデータを使用でき、かつ自動的に、そのユーザによるコンテンツデータの使用料を課金できるという効果がある。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るデータ処理装置の概略構成を示すブロック図である。

【図２】本発明に係るＩＰＭＰデータのデータ構造を示す図である。

【図３】一般的な配信システムの全体構造の一例を示す図である。

【図４】本発明の実施の形態に係るデータ配信システム（課金装置無し）における各装置間のデータの流れを説明する図である。

【図５】本発明の実施の形態に係るデータ配信システム（課金装置あり）における各装置間のデータの流れを説明する図である。

【図６】本実施の形態に係る課金／決済を行うために必要となるデータの一例を示す図である。

【図７】本実施の形態に係る課金／決済を行うために必要となるデータの一例を示す図である。

【図８】本発明の実施の形態に係るデータ処理装置の動作を説明するためのフローチャートである。

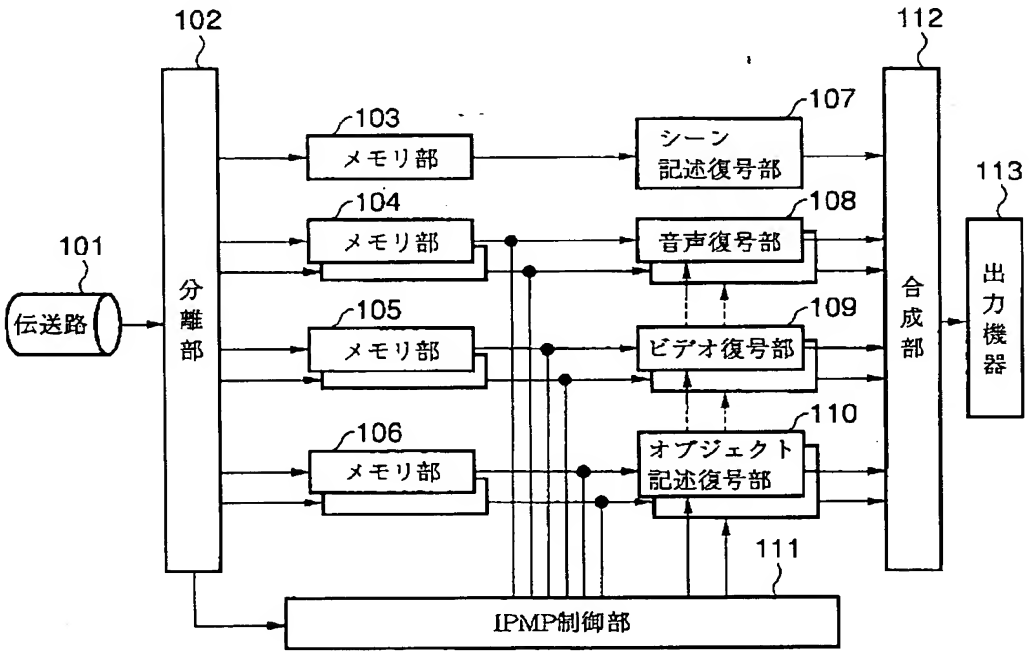
【図９】本発明の実施の形態に係る証明書発行装置の動作を説明するためのフローチャートである。

【図１０】本発明の実施の形態に係る課金装置の動作を説明するためのフローチャートである。

【図１１】本発明の実施の形態に係るデータ変換装置の動作を説明するためのフローチャートである。

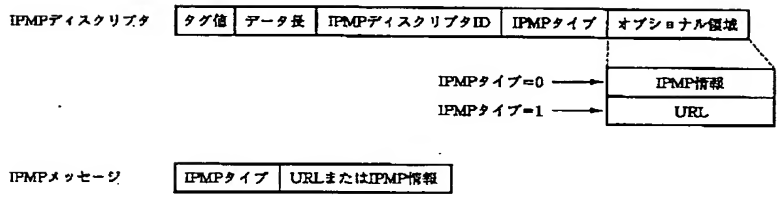
【図１２】本発明の実施の形態に係るコンテンツサーバの動作を説明するためのフローチャートである。

【図１】

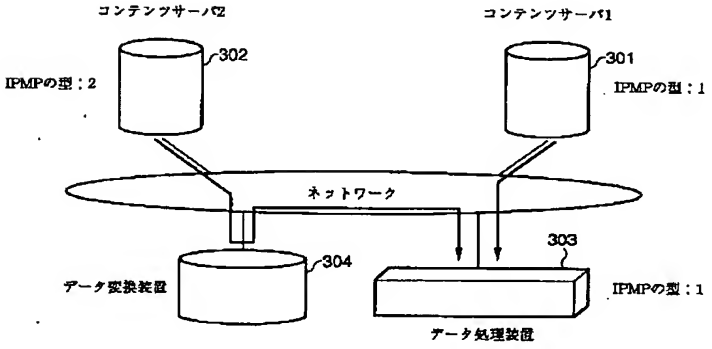


制御ポイント

【図２】



【図３】

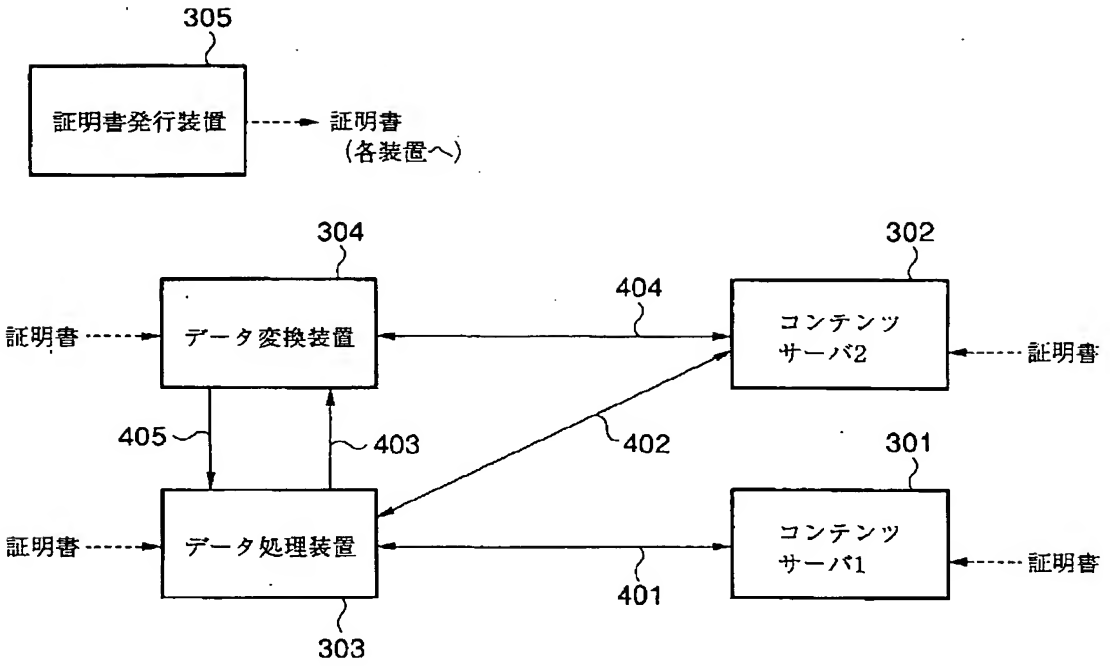


【図６】

ユーザ名	ユーザID	送信コンテンツID	送信日時	鍵データの送信
ABC	00001	100000	2000/01/01	0x1234567
DEF	00002	200000	2000/01/02	無し
……	……	……	……	

←1ブロック

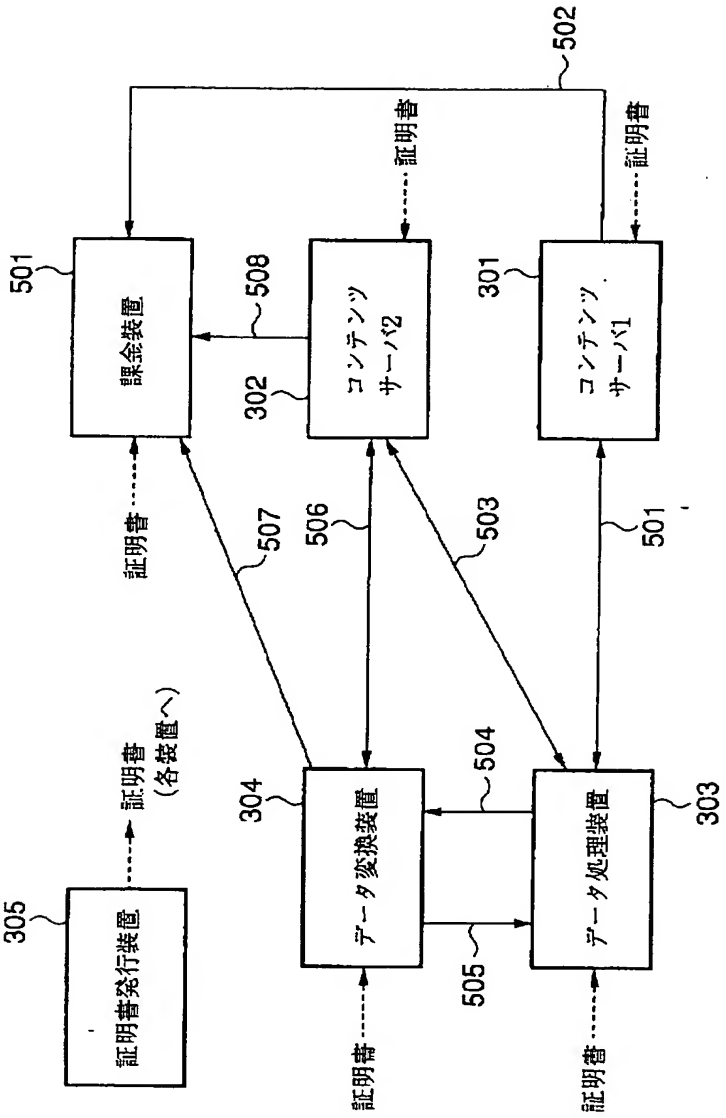
【図４】



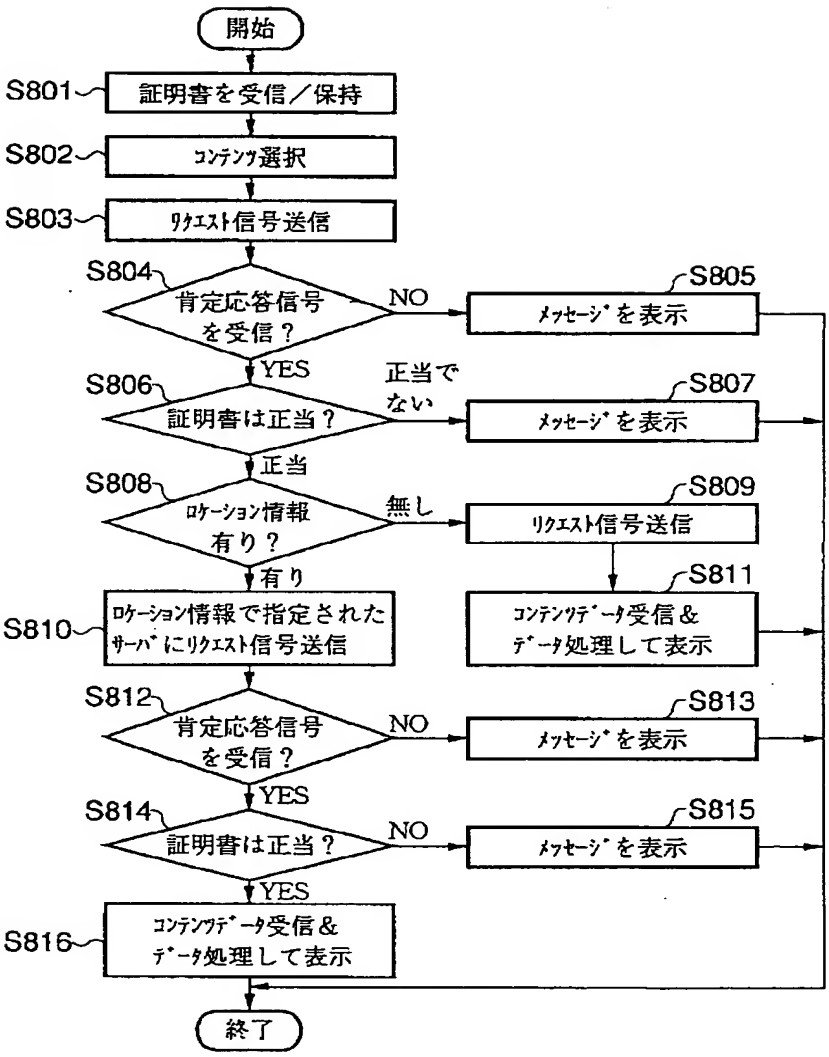
【図７】

ユーザ名	ユーザID	送信コンテンツID	送信日時	変換データ量	変換したIPMPタイプ	鍵データの送信
ABC	00001	100000	2000/01/01	10MByte	2→1	0x7654321
DEF	00002	200000	2000/01/02	20MByte	1→2	無し
.....	.....	.....	.....	.....	.....	.....

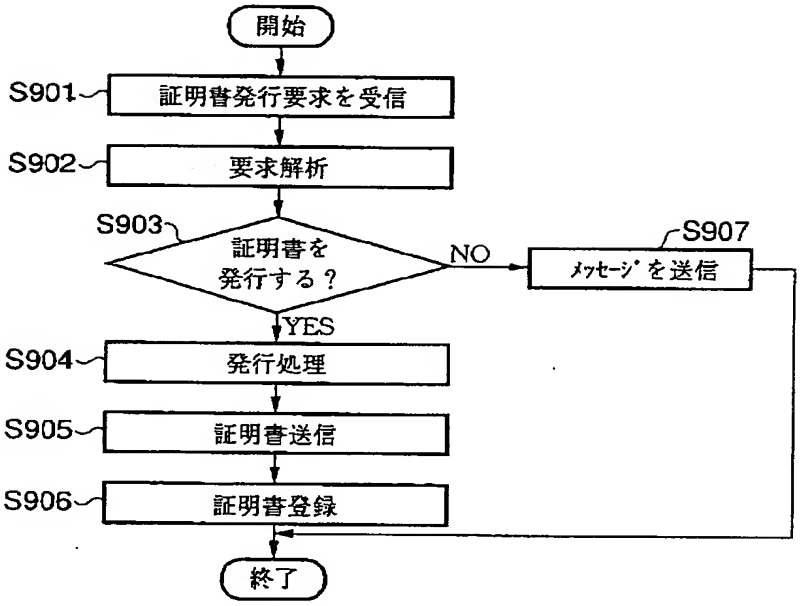
【図５】


502
証明書
証明書
501
課金装置
508
コンテンツサーバ2
302
301
コンテンツサーバ1
証明書
507
506
503
501
証明書（各装置へ）
304
データ変換装置
504
データ処理装置
303
305
証明書発行装置
505
証明書
証明書

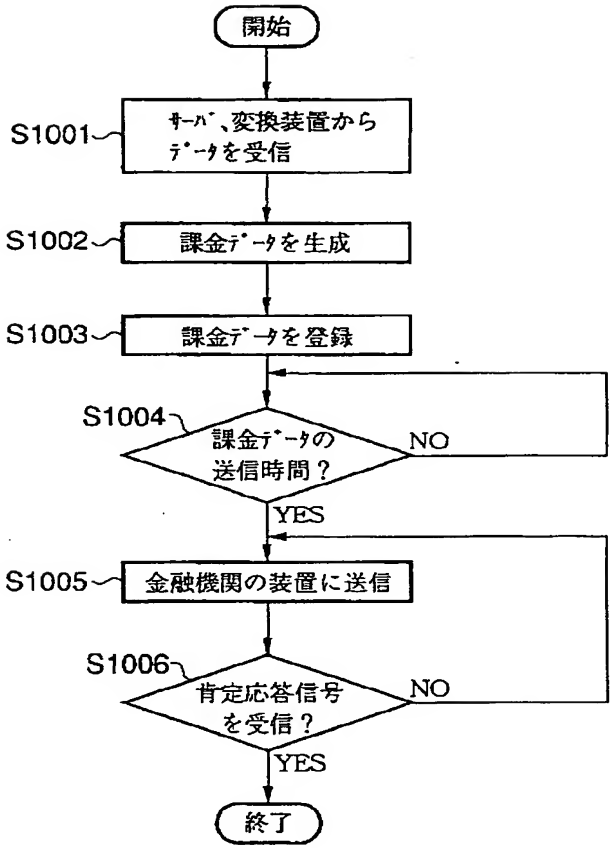
【図８】


開始
S801
証明書を受信／保持
S802
ｺﾝﾃﾝﾂ選択
S803
ﾘｸｴｽﾄ信号送信
S804
肯定応答信号を受信？
NO
S805
ﾒｯｾｰｼﾞを表示
YES
S806
証明書は正当？
正当でない
S807
ﾒｯｾｰｼﾞを表示
正当
S808
ﾛｹｰｼｮﾝ情報有り？
無し
S809
ﾘｸｴｽﾄ信号送信
有り
S810
ﾛｹｰｼｮﾝ情報で指定されたｻｰﾊﾞにﾘｸｴｽﾄ信号送信
S811
ｺﾝﾃﾝﾂﾃﾞｰﾀ受信＆ﾃﾞｰﾀ処理して表示
S812
肯定応答信号を受信？
NO
S813
ﾒｯｾｰｼﾞを表示
YES
S814
証明書は正当？
NO
S815
ﾒｯｾｰｼﾞを表示
YES
S816
ｺﾝﾃﾝﾂﾃﾞｰﾀ受信＆ﾃﾞｰﾀ処理して表示
終了

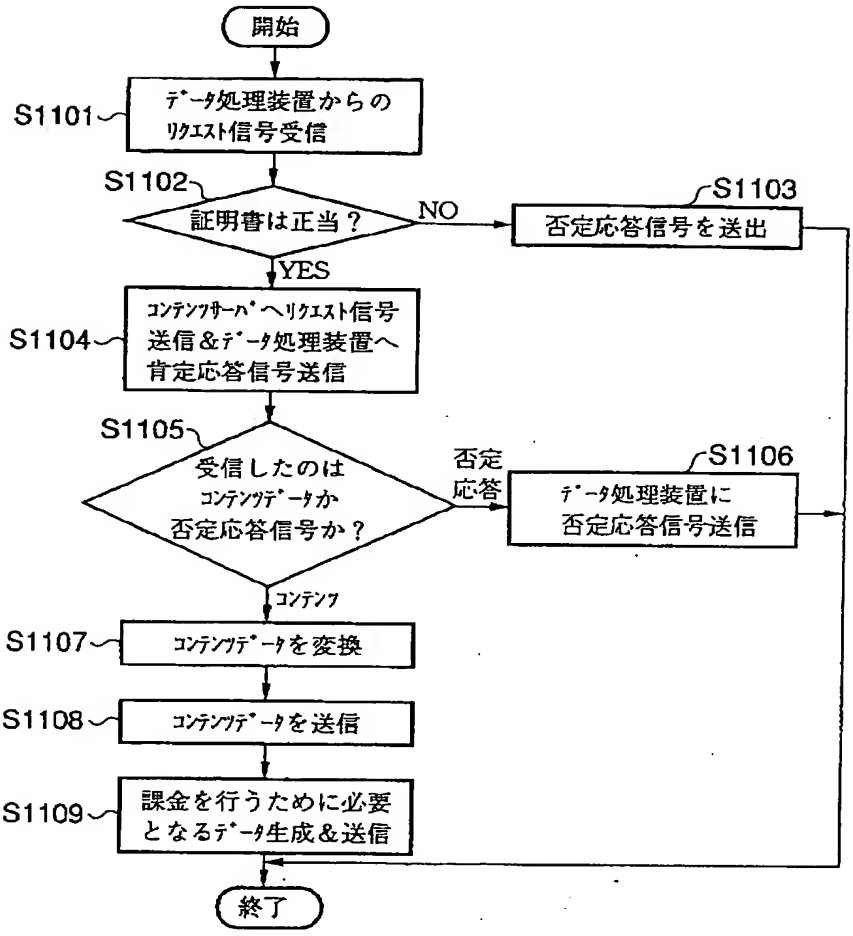
【図９】


開始
S901
証明書発行要求を受信
S902
要求解析
S903
証明書を
発行する？
NO
S907
ﾒｯｾｰｼﾞを送信
YES
S904
発行処理
S905
証明書送信
S906
証明書登録
終了

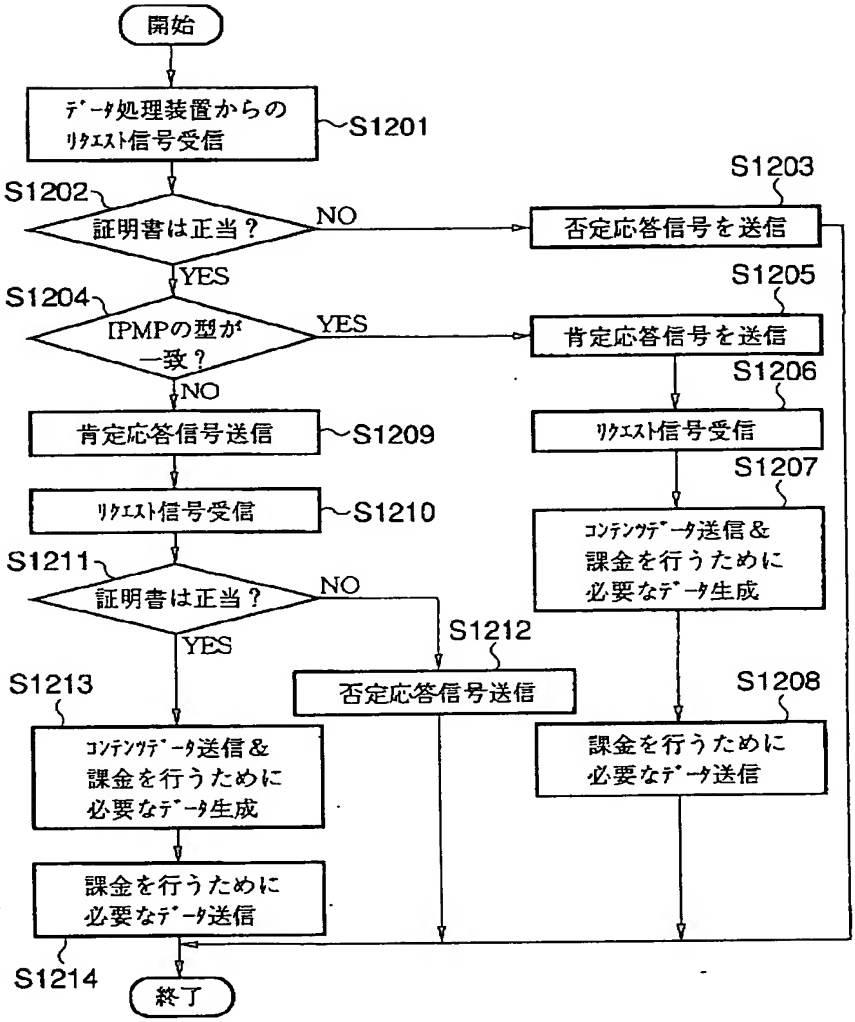
【図１０】


開始
S1001
ｻｰﾊﾞ、変換装置から
ﾃﾞｰﾀを受信
S1002
課金ﾃﾞｰﾀを生成
S1003
課金ﾃﾞｰﾀを登録
S1004
課金ﾃﾞｰﾀの
送信時間？
NO
YES
S1005
金融機関の装置に送信
S1006
肯定応答信号
を受信？
NO
YES
終了

【図１１】


開始
S1101
ﾃﾞｰﾀ処理装置からの
ﾘｸｴｽﾄ信号受信
S1102
証明書は正当？
NO
S1103
否定応答信号を送出
YES
S1104
ｺﾝﾃﾝﾂｻｰﾊﾞへﾘｸｴｽﾄ信号
送信&ﾃﾞｰﾀ処理装置へ
肯定応答信号送信
S1105
受信したのは
ｺﾝﾃﾝﾂﾃﾞｰﾀか
否定応答信号か？
否定
応答
S1106
ﾃﾞｰﾀ処理装置に
否定応答信号送信
ｺﾝﾃﾝﾂ
S1107
ｺﾝﾃﾝﾂﾃﾞｰﾀを変換
S1108
ｺﾝﾃﾝﾂﾃﾞｰﾀを送信
S1109
課金を行うために必要
となるﾃﾞｰﾀ生成&送信
終了

【図１２】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	１４２	Ｇ０６Ｆ　17/60	１４２
	３０２		３０２Ｅ
	３３２		３３２